VANET 상에서의 이동성을 고려한 안전한 메시지 인증기법

서화정* · 김호원**

A Secure Mobile Message Authentication Over VANET

Hwa-jeong Seo* · Ho-won Kim**

이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.2010-0026621).

요 약

지능형 차량 네트워크(VANET)는 무선통신을 이용하여 차량 간(V2V, Vehicle to Vehicle), 차량과 노변장치 간(V2I, Vehicle to Infrastructure)의 통신을 제공하는 네트워킹 기술이다. 현재 VANET통신은 자동차산업의 급속한 발전과 차량자동화로 인하여 산업계와 학계를 중심으로 연구가 활발히 진행되고 있다. VANET을 통해 유통되는 차량의 속도, 가속도, 도로 및 환경 모니터링정보는 운전자에게 안전운전과 관련된 서비스를 제공하는 분야로써 통신에서의 보안은 필수적인 요건이다. 지금까지 안전한 메시지 인증을 위한 많은 인증프로토콜들이 제시되어 왔다. 그 중에서도 Jung에 의해 제안된 VANET 알고리즘은 데이터베이스 검색 알고리즘인 블룸 필터를 RAISE 알고리즘에 적용하여 차량 밀집환경에서의 인증에 보다 효율적인 알고리즘을 제안하였다. 하지만 RAISE에서 사용한 k-anonymity는 정확한 차량의 ID정보를 얻기 위해 모든 메시지에 대해 전수조사 연산을 수행해야 하므로 차량의 수가 증가함에 따라 해시연산량이 지수적으로 증가한다. 또한 핸드오버가 발생하는 경우 완벽한 키전달 알고리즘을 제공하지 못한다. 본 논문에서는 RSSI기반 속도 및 거리 추정 알고리즘을 사용하여 사용자의 ID를 위치화하며 프로토콜의 핸드오버부분의 오류를 수정하여 안전하고 효율적인 알고리즘을 제공한다.

ABSTRACT

Vehicular Ad Hoc Network(VANET) using wireless network is offering the communications between vehicle and vehicle(V2V) or vehicle and infrastructure(V2I). VANET is being actively researched from industry field and university because of the rapid developments of the industry and vehicular automation. Information, collected from VANET, of velocity, acceleration, condition of road and environments provides various services related with safe drive to the drivers, so security over network is the inevitable factor. For the secure message authentication, a number of authentication proposals have been proposed. Among of them, a scheme, proposed by Jung, applying database search algorithm, Bloom filter, to RAISE scheme, is efficient authentication algorithm in a dense space. However, k-anonymity used for obtaining the accurate vehicular identification in the paper has a weak point. Whenever requesting the righteous identification, all hash value of messages are calculated. For this reason, as the number of car increases, a amount of hash operation increases exponentially. Moreover the paper does not provide a complete key exchange algorithm while the hand-over operation. In this paper, we use a Received Signal Strength Indicator(RSSI) based velocity and distance estimation algorithm to localize the identification and provide the secure and efficient algorithm in which the problem of hand-over algorithm is corrected.

키워드

RSSI, VANET, 익명성, Hand Over

Key word

RSSI, VANET, Anonymity, Hand Over

* 준회원 : 부산대학교 컴퓨터공학과 석사과정 (hwajeong@pusan.ac.kr)
** 종신회원 : 부산대학교 컴퓨터공학과 교수

접수일자 : 2011. 02. 08
심사완료일자 : 2011. 03. 07

Ⅰ. 서 론

차량에 설치된 무선 통신기기를 통한 지능형 차량 간 그리고 차량과 노변장치간의 통신을 VANET (Vehicle Ad-hoc Network)이라고 한다. VANET은 운전자의 안전을 보장을 위해 활용되는 기술로써 산업계와 학계를 중심으로 연구가 활발히 진행되고 있다. 운전자는 VANET을 통해 자신의 자동차의 속도, 가속도, 위치 정보를 차량에 탑재된 OBU(On Board Unit)를 통해 RSU(Road Side Unit)로 전달한다. RSU에서는 도로의 상태정보인 교통사고 발생, 갑작스런 기상 변화, 도로의 결빙 상태 그리고 상대방 차량의 정보를 통합하여 안전운전에 필요한 정보를 운전자에게 제공한다.[1]. VANET은 차량과 노변장치간의 통신과 노변장치와 서버간의 통신으로 구성된다. 전자의 경우에는 주로 센싱정보에 대한 교환을 통해 환경 및 차량의 모니터링에 사용되며 후자의 경우에는 RSU에 종합된 정보를 미들웨어단으로 전송한 뒤 가공 및 수정하여 운전자에게 필요한 정보를 제공한다. 따라서 유통되는 정보의 중요도를 고려해 볼 때 안전한 보안통신이 필수적이다.

2008년에는 Zhang에 의해 RSU와 OBU간의 안전한 정보교환을 제공하는 RAISE스킴이 제안되었다. 이는 RSU에 비해 자원이 한정적인 OBU 상에서의 통신량과 계산량을 줄이고 대신 RSU에서의 계산 및 통신량을 증가시킴으로써 차량이 밀집된 환경에서 효율적인 메시지 인증이 가능하다[4]. 하지만 본 기법은 차량들이 밀집된 환경에서 보내는 메시지의 인증을 위해 해시체인을 사용함으로써 메시지의 수가 증가함에 따라 인증메시지의 길이도 함께 증가하는 문제가 있다.

최근에는 차량이 밀집된 환경에서도 효율적인 통신이 가능한 기법이 Jung에 의해 제시되었다[2]. 해당 기법은 블룸 필터 알고리즘을 사용하여 차량의 수에 관계없이 일정한 크기의 HMAC 결과값을 유지할 뿐 아니라 타임스탬프를 통한 Replay Attack을 방지한다[3]. 하지만 해당 스킴은 RAISE을 기반으로 작성되어 k-anonymity를 통한 익명성 보장기법을 사용한다. 이는 RSU에서 사용자의 ID를 확인 시 모든 메시지에 대한 해시전수조사를 수행해야 하는 문제가 있다. 또한 핸드오버기능은 프로토콜적 오류가 있어 완벽한 키교환이 일어날 수 없다.

따라서 본 논문에서는 RSSI기반 아이디 방식을 통해 k-anonymity를 통한 인증을 대체한다[6]. 또한 Jung에 의해 제안된 기법의 핸드오버상의 문제점을 새로운 프로토콜 제안을 통해 해결한다.

본 논문은 다음과 같이 구성된다. 2장에서는 Jung 의 기법, k-anonymity, CRSD의 특성에 대해 알아본다. 3장에서는 제안하는 시스템 모델 및 기법에 대해 설명한다. 4장에서는 제안하는 기법의 안전성과 효율성을 분석하고 마지막으로 5장에서는 본 논문의 결론을 내린다.

Ⅱ. 관련 연구

2.1. Jung의 기법

Jung의 기법은 기존의 PKI기반의 메시지 인증기법사용 시 차량이 밀접한 상황에서 통신량과 계산량이 증가하는 문제를 해결하기 위해 개발되었다. 기본적인 골격은 RAISE 기법이다. 따라서 RSU를 통해 통합된 메시지는 k-anonymity 특성을 사용하여 각 차량의 익명성을 보장하며 차량의 인증이 수행된다. 기존 RAISE 기법에 비해 개선된 사항은 블룸 필터를 인증통합메시지에 적용하여 차량의 수에 관계없이 일정한 크기의 메시지를 유지하는 점이다. 이를 통해 밀집된 차량 환경에도 효율적인 통신이 가능하다.

2.1.1. Jung기법의 상세

해당 기법은 차량들 간의 보안통신을 위해 아래와 같은 절차로 수행된다.

2.1.1.1. 대칭키 설립

Diffie-Hellman 키 교환 프로토콜을 사용하여 차량의 OBU와 RSU 간의 대칭키를 공유한다[7].

2.1.1.2. 해쉬통합 (Hash Aggregation)

i번째 메시지를 송신하는 차량은 RSU와 공유한 키를 이용하여 자신의 아이디와 메시지와 그 서명값 $ID_i \| M_i \| HMAC_{K_i}(ID_i \| M_i)$를 RSU와 다른 차량에게 전송하게 된다. 이를 전송받은 RSU는 자신이 가진 ID-Table에 해당 ID가 존재하는지 서명값을 확인 후 정당한 메시지인 경우 ID와 메시지의 쌍을 블룸필터

($BAggt = H(ID_1 \| M_1) \| ... \| H(ID_n \| M_n)$)에 삽입시키다. 해당 메시지는 RSU의 개인키로 서명되어 차량에게 전송된다.

2.1.1.3. 검증

메시지를 송신 받은 차량은 블룸 필터로 통합된 메시지의 서명값($BAggt \| (BAggt)_{k_{RSU}}$)을 검증한 후 수신한 메시지 $ID_i \| M_i \| HMAC_{K_i}(ID_i \| M_i)$의 HMAC값이 블룸 필터에 존재하는지 확인한다.

2.1.1.4. 핸드오버

차량이 기존의 RSU의 도메인을 벗어나 다른 RSU에 속하게 되는 경우 핸드오버과정을 통해 키교환없이 통신이 가능하다.

2.1.1.4.1. 메시지 수신차량의 도메인 이동

메시지 수신차량이 기존의 도메인에서 다른 도메인의 RSU로 이동하게 될 경우 기존의 RSU로부터 블룸 필터를 제공받음과 동시에 공개키값으로 암호화된 기존의 RSU와의 키값을 제공받게 된다.

$$BAggt \| (BAggt)_{SK_{RSU}}, Enc_{K_{RSU}}(K_{RSU,SV})$$

이를 전송받은 새로운 도메인의 RSU는 자신의 개인키로 차량의 키값을 추출하며 동시에 블룸 필터에 exclusive-or연산을 하여 현재의 블룸 필터에 포함시키게 된다.

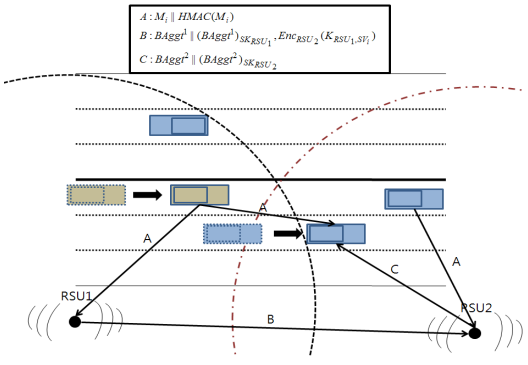

그림 1. Jung의 기법에서의 메시지 수신차량의 도메인 이동

Fig 1. Domain transfer of message recipient in Jung scheme

여기서 차량이 그림 1에서와 같이 일방향성의 길을 간다면 수신차량의 다음 RSU를 예측하는 것이 가능하다. 하지만 실질적으로 도로상에는 교차로가 있으므로 수신차량이 이동할 RSU를 찾는다는 것은 교차로의 모든 RSU에게 query를 날려서 차량의 위치를 확인한 후 핸드오버 과정을 수행해야 한다.

2.1.1.4.2. 메시지 송신차량의 도메인 이동

메시지 송신차량의 도메인이 변경되는 경우 변경된 도메인의 RSU는 송신차량의 메시지를 자신의 블룸 필터에 포함한 후 차량의 키값을 변경전의 도메인의 공개키로 암호화하여 전송하게 된다. 이를 전송받은 변경전의 도메인은 자신의 개인키로 차량의 키값을 추출하며 동시에 블룸 필터에 exclusive-or연산를 하여 현재의 블룸 필터에 포함시키게 된다. 하지만 송신차량이 이동된 RSU2는 해당 차량이 이전에 어떤 RSU1에 속했었는지에 대한 정보가 없으므로 이동된 차량의 인증이 불가능하며 또한 RSU2는 RSU1과 차량의 키값을 알 수 없는데 기법상의 B에서 키값을 전송한다고 나와 있는 부분은 프로토콜적 오류이다.

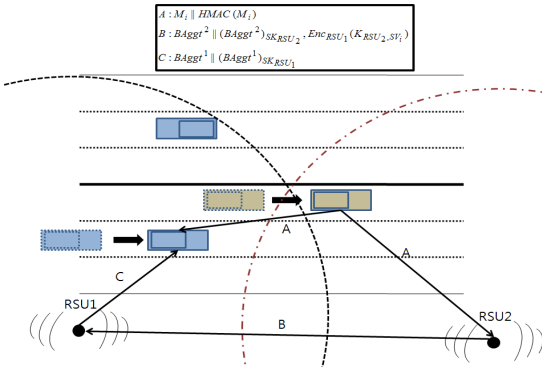

그림 2. Jung의 기법에서의 메시지 송신차량의 도메인 이동

Fig 2. Domain transfer of message sender in Jung scheme

2.2. 블룸 필터

블룸 필터는 1970년 Burton H. Bloom에 의해 제안된 확률적인 특성을 가지는 자료구조이다[3]. 해당 자료구조는 주어진 집합에 찾고자 하는 원소가 포함되어 있는지 판단하기 위해 포함되는 원소의 bit를 해시 함수로 계산한 후 자료구조에 포함시키는 형식으로 동작한다.

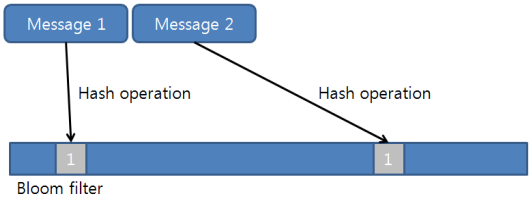

그림 3. 블룸 필터
Fig 3. Bloom filter

사용가능한 함수는 Insert와 Check가 있다. Insert 함수는 입력값으로 메시지의 해시값을 받아 해쉬의 결과값의 위치에 있는 블룸 필터 값을 1로 바꾼다. 블룸 필터의 값을 확인하기 위해서는 Check함수를 사용하는데 해당함수는 연산 시 하나라도 0이 되는 블룸 필터값이 있다면 메시지가 포함되지 않는다는 것을 의미한다. 블룸 필터는 Union과 Intersection 속성을 만족한다. Union은 블룸 필터 간의 exclusive-or연산을 통해 양쪽에 속한 원소값을 하나의 블룸 필터로 통합하는 기능이다. Intersection은 두 개의 블룸 필터의 크기가 동일한 경우 교집합에 해당하는 원소만을 통해 새로운 집합을 생성한다.

2.3. k-anonymity

K개의 PID(Pseudo-ID)를 사용하여 통신을 하게 될 경우 공격자는 PID를 통해 현재 VANET상에서 통신하는 차량의 ID를 확인하는 것이 불가능하다. 그 이유는 PID가 차량의 ID정보를 포함하지 않기 때문이다. 반면에 RSU의 경우 자신이 가진 모든 ID값을 전수조사를 통해 차량의 ID값을 확인하는 것이 가능하다. 따라서 차량은 익명성을 보장받는 가운데 RSU와 안전한 통신이 가능하게 된다. 하지만 전수조사로 인한 부하가 발생하는 문제점이 있다.

2.4. CRSD(Cooperative RSS-based Sybil Detection)

CRSD는 주위의 여러 노드간의 RSSI(Received signal strength indication)정보를 이용하여 노드들간의 상대적인 거리를 계산하여 Sybil attack을 탐지하는 기법이다[5]. 여기서 Sybil Attack이란 하나의 존재가 다른 존재로 가장하여 네트워크의 Routing에 혼란을 가져옴으로써 성능을 저하시키는 공격을 의미한다. 알고리즘은 그림 4와 같이 각자의 위치에서 측정되는 RSSI값을 통해 노드의 위치를 탐지하게 된다. 만약 노드 서로간의 RSSI값을 비교하여 동일한 RSSI값을 가진 노드가 2개 이상발생할 경우 Sybil attack이 발생한 것으로 간주한다.

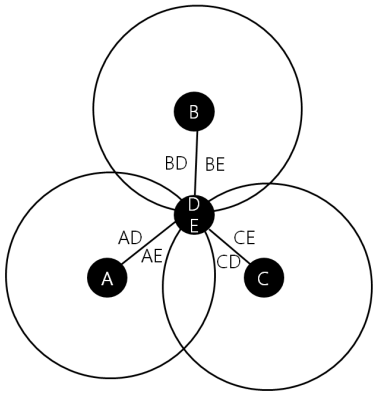

그림 4. CRSD 기법
Fig 4. CRSD Technique

2.5. RSSI기반 거리,계산 알고리즘[6]

표 1는 표 2, 3에서 사용될 용어에 대한 설명이다.

표 1. 용어 정리
Table 1. Terms used in Table 2, 3.

표 기	정 의
n	신호 전파 상수
d	거리
A_R:	1미터상에서의 RSSI 값
V	속도
T	RSSI 측정주기
A	가속도

RSSI값을 사용하면 식 (2)와 같이 거리의 식을 나타낼 수 있다. RSSI값은 거리에 따라 일정하게 감소하므로 이를 통해 거리를 계산하는 것이 가능하다.

표 2. RSSI와 거리식
Table 2. Equation of distance and RSSI

계산할 값	정의
RSSI값	$RSSI = -(10n\log d + A_R)$ (1)
RSSI를 통한 거리 계산	$d = 10^{-\frac{RSSI + A_R}{10n}}$ (2)

또한 RSSI를 통한 거리 값을 시간에 따라 일정한 간격으로 측정시 거리의 변화량인 속도와 시간에 따른 속도 변화량인 가속도를 계산할 수 있다.

표 3. RSSI를 통한 속도 및 가속도식
Table 3. Equation of velocity and acceleration using RSSI

계산된 값	정 의
속도	$\triangle d_n = d_{n+1} - d_n$ (3) $V = \frac{\Delta d_n}{T}$ (4)
가속도	$\triangle V_n = V_{n+1} - V_n$ (5) $A = \frac{\Delta V_n}{T}$ (6)

Ⅲ. 제안하는 기법

VANET은 AS(Application Server)와 RSU(Road Side Units)간의 통신, RSU와 각 차량 간의 통신으로 구분된다. 본 논문에서 제안하는 기법은 RSU와 차량간의 통신으로 제한하며 AS와 RSU는 물리적으로 안전하게 보호받는다고 가정한다.

3.1. 용어정리

표 4. 용어정리
Table 4. Description of terms

표 기	정 의
RSU^j	j번째 영역의 RSU
SV_i^j	j번째 영역에서 메시지를 송신하는 i번째 차량
RV_i^j	j번째 영역에서 메시지를 수신하는 i번째 차량
$K_{A,B}$	RSU A와 차량 B간에 교환한 대칭키
$HMAC_{K_{A,B}}(C)$	C의 HMAC을 $K_{A,B}$로 계산한 값
$(A)_{SK_B}$	A를 B의 개인키로 서명한 값
$BCAggt$	각 메시지의 해쉬값을 삽입한 블룸 필터값
$Enc_{K_B}(A)$	A를 B의 공개키로 암호화한 값
K_{RSU^j}	RSU^j의 공개키
G_i	i번째 영역의 ID
V_i	i번째 차량의 속도
L_i	i번째 차량의 위치정보

3.2. 제안하는 기법

제안하는 기법은 RSU1_Assistant와 RSU1에서 측정된 RSSI값을 이용하여 계산된 차량의 위치 및 속도를 통해 차량의 ID를 생성한다. 그림 5는 제안하는 기법의 대칭키 설립부터 차량의 메시지 전송 그리고 해쉬통합을 통한 검증과정을 나타낸다.

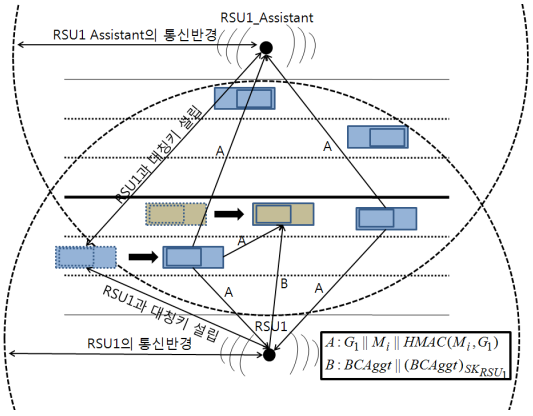

그림 5. 제안하는 기법의 해쉬통합 및 검증
Fig 5. Hash Aggregation and authentication in proposed scheme

3.2.1. 대칭키 설립

j번째 영역에 i번째 차량 V_i^j가 RSU1과 RSU1_Assistant에게 메시지를 전송하면 RSU는 받은 RSSI값을 이용하여 차량 V_i^j의 상대적인 거리를 계산한다. 동시에 차량과 RSU간의 Diffie-Hellman 키교환 프로토콜이 수행된다. 키교환은 3 Hand shake로 수행된다 따라서 차량의 RSSI 값이 RSU1와 RSU1_Assistant에서 각각 두 번씩 탐지된다. 첫 번째 전송된 RSSI를 통해 위치정보를 측정하고 두 번째 위치정보를 통해 차량 V_i^j의 속도를 계산한다. 또한 누적된 속도값을 이용하여 차량의 가속도를 연산한다. 계산된 거리와 속도는 차량 마다 가지게 되는 고유한 값이므로 차량을 지칭하는 ID로 대체가능하다. 키교환이 이루어 지고 난 뒤에 차량은 메시

지 $G_1 \| M_i \| HMAC(G_1 \| M_i)$를 RSU에게 전송한다. 여기서 보내지게 되는 메시지는 자신이 속한 RSU의 Group ID값과 Message 그리고 Group ID와 Message를 해쉬연산한 값을 포함한다. 이를 전송받은 RSU는 차량의 RSSI값을 표 5의 Key Table과 비교해서 HMAC값이 일치하는지 검증한다. 이때 참조되는 Key Table의 내용은 일정시간 동안 갱신되지 않을시 자동으로 삭제된다.

표 5. Key Table
Table 5. Key Table

RSU로부터 위치	RSU_ASSISTANT로부터 위치	속도	가속도	KEY
L_1	L_{1a}	V_1	A_1	K_1
L_2	L_{2a}	V_2	A_2	K_2
L_3	L_{3a}	V_3	A_3	K_3
• • •	• • •	• • •	• • •	• • •
L_k	L_{ka}	V_k	A_k	K_k

3.2.2. 해쉬통합(Hash Aggregation)

RSU와 차량 간에 키교환이 이루어지고 나면 차량은 자신이 보내고자 하는 메시지 $G_1 \| M_1 \| HMAC(G_1 \| M_1)$를 전송하게 된다. 메시지의 구성은 자신이 위치한 RSU의 Group ID값 G_1, 자신의 메시지 그리고 HMAC을 취한 값을 포함한다. 이를 전송받은 RSU와 RSU_Assistant는 해당 차량의 위치정보, 속도, 가속도를 RSSI를 기반으로 계산하여 정확한 차량과 키값을 확인하게 된다.

만약 해쉬값이 차량의 키값으로 확인이 된다면 블룸필터에 메시지를 삽입하게 된다. 모든 차량으로부터 받은 메시지를 통합하여 블룸 필터가 완성되면 RSU는 차량들에게 필터정보를 전송하게 된다. 전송되는 정보는 필터와 필터의 서명값 $BCAggt^1 \| (BCAggt^1)_{SK_{RSU^1}}$이다.

3.2.3. 검증

메시지 $BCAggt^1 \| (BCAggt^1)_{SK_{RSU^1}}$를 전송받은 차량은 RSU의 공개키를 통해 서명값을 인증한다. 만약 서명값이 정당한 값이라면 $G_1 \| M_1 \| HMAC(G_1 \| M_1)$의 메시지값을 해쉬연산하여 메시지가 필터에 포함되는지 확인한다.

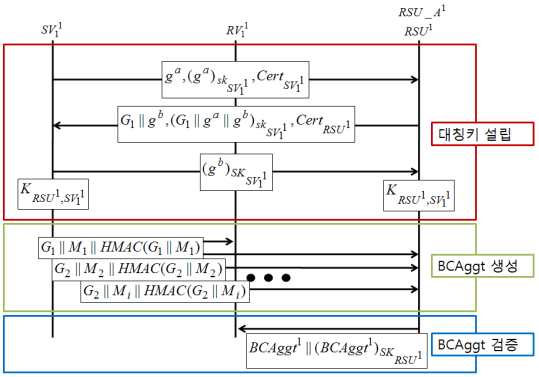

그림 6. 해쉬통합 및 검증 프로토콜
Fig 6. Hash Aggregation and Authentication Protocol

3.2.4. 핸드오버

Jung에 의해 제안된 핸드오버의 경우 이동된 차량의 확인부터 인증과정에 대한 명확한 프로토콜이 제안되지 않았으며 프토콜적 오류가 존재하여 핸드오버가 불가능하다. 따라서 본 논문에서는 도메인 이동이 일어나는 경우에도 수신차량의 키값 교환 및 filter갱신이 가능한 프로토콜을 고안하였다.

3.2.4.1. 수신차량의 도메인 이동

메시지를 수신하는 차량의 도메인이 변경되는 경우 해당차량은 변경된 도메인에서 메시지를 보내게 된다. 이를 전송받은 RSU2는 자신과 다른 Group ID를 가진 해당 차량이 다른 RSU로부터 이동해온 차량임을 확인하고 새로운 Group ID를 전송해주게 된다. 이를 전송받은 차량은 메시지를 받았다는 의미로 응답을 해주게 된다. 여기서 총 2번의 메시지 전송이 일어나므로 RSU2와 RSU2_Assistant는 차량의 RSSI값을 통해 위치 및 속도 정보계산이 가능하다. 해당 정보는 Group ID를 통해 판단된 RSU1의 공개키로 암호화하여 RSU1에게 보내지며 이를통해 차량을 판단할 수 있다. 예를들어 차량이 RSU1에서 3차선 위에서 차량이 50km로 주행 중이었다면 RSU2의 위치 및 속도 정보를 통해 현재 3차선 및 약 50km로 주행중인 차량 정보를 판단한다. 차량정보를 확인한 RSU1은 해당 차량의 키값을 RSU2에게 전송해주며 이를 받은 RSU2는 필터정보 및 키값을 차량에게 전

송해준다.

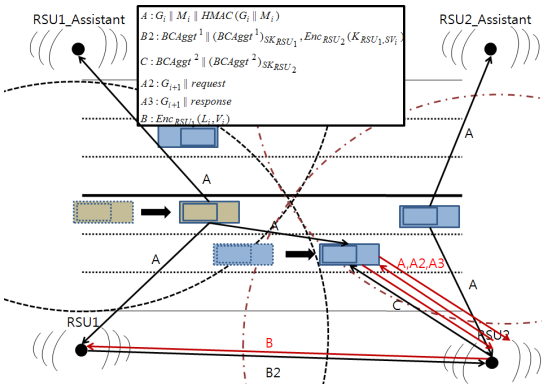

그림 7. 메시지 수신차량의 도메인 이동
Fig 7. Domain transition of message recipient

그림 8은 수신차량의 핸드오버를 흐름도로 나타낸 것이다. 기법은 도메인이 변경되는 부분과 새로운 차량을 인증하는 부분 그리고 블룸 필터를 검증하는 부분으로 구성된다.

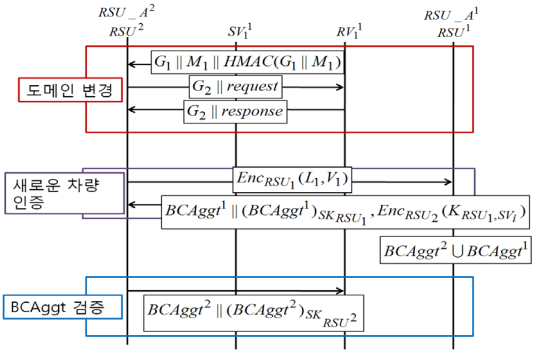

그림 8. 핸드오버(메시지 수신차량의 도메인 이동)
Fig 8. Hand over(Domain transfer in message recipient)

3.2.4.2. 송신차량의 도메인 이동

RSU2는 자신의 Group ID와 다른 메시지가 전송된 경우 메시지 요청과 함께 자신의 Group ID를 전송하게 된다. 이를 받은 차량은 변경된 Group ID와 응답 메시지를 전송하게 된다. 두 번의 메시지를 전송받은 RSU2와 RSU2_Assistant는 차량의 위치와 속도정보를 알 수 있고 이를 RSU1에게 전송한다. 이를 전달받은 RSU1는 현재 위치 및 속도 정보에 만족하는 키값을 RSU2에게 RSU1의 공개키로 암호화하여 전송한다. 이를 전송받은 RSU2는 RSU1에게 전송받은 메시지를 보내주며 RSU1에서는 해쉬 통합을 거쳐 목적지 차량에게 전송되게 된다.

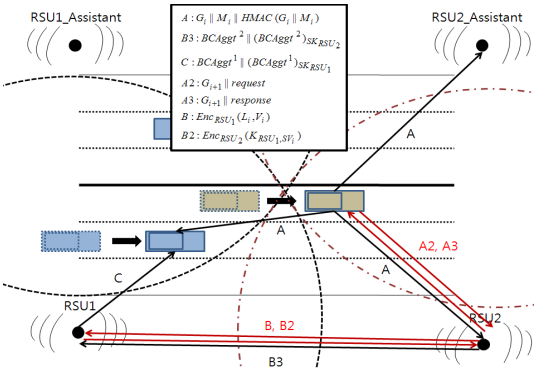

그림 9. 메시지 송신차량의 도메인 이동
Fig 9. Domain transfer in message sender

그림 10은 송신차량의 핸드오버를 흐름도로 나타낸 것이다. 기법은 도메인이 변경되는 부분과 새로운 차량을 인증하는 부분 그리고 필터를 갱신하는 과정을 포함한다.

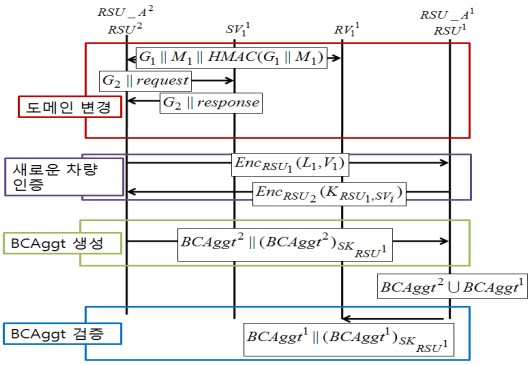

그림 10. 핸드오버(메시지 송신차량의 도메인 이동)
Fig 10. Hand over(Domain transfer in message sender)

3.2.5. RSSI를 통한 차량확인

그림 6의 키교환단계의 첫 번째 과정에서 $g^a, (g^a)_{sk_{SV_1^1}}, Cert_{SV_1^1}$을 등록하고자 하는 차량으로부터 전달받게 된다. 이때 RSU와 RSU_Assistant에서는 해당 차량의 RSSI값을 등록한다. 그리고 RSU에서는 다시 차

량쪽으로 $G_1 \| g^b, (G_1 \| g^a \| g^b)_{sk_{SV_1}}, Cert_{RSU^1}$를 전송한다. 이를 전송받은 차량은 Diffie-hellman을 통해 차량과 RSU사이의 키를 생성한다. 동시에 차량은 $(g^b)_{SK_{SV_1}}$을 RSU에게 전달해준다. 이때 RSU는 전송된 메시지의 RSSI값을 통해 차량의 속도를 계산하며 키 테이블에 저장하게 된다. 만약 RSSI의 불안정성으로 인해 구분이 힘든 경우에는 차량에 부여된 난수값 g^b의 서명값을 확인하여 차량을 정확히 판단하는 것이 가능하다. 일단 차량의 키가 분배된 이후에는 차량은 일정한 주기를 가지고 RSU와 실시간으로 통신하게 된다. 차량의 확인은 그림 11과 같은 순서로 이루어 진다. 먼저 주기를 통해 해당 차량을 확인하며 동일한 주기가 존재하는 경우 RSSI를 통한 위치, 속도, 가속도정보를 추가적으로 사용한다. 만약 이 경우에도 정확한 차량을 찾지 못하면 전수조사를 통해 차량을 파악하게 된다.

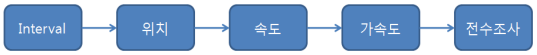

그림 11. 차량 확인 과정
Fig 11. Procedure of vehicle verification.

Ⅳ. 안전성 및 효율성 분석

4.1. 안전성

4.1.1. 인증

RSU는 블룸 필터와 전송되어진 메시지의 HMAC값을 통해 메시지를 보낸 차량의 인증이 가능하다. RSU는 메시지의 HMAC값이 키 Table에 등록되어 있는 경우 필터에 삽입하게 된다. 따라서 RSU로부터 필터값을 전송받은 차량은 필터를 확인하여 메시지를 인증한다.

4.1.2. 메시지 무결성

메시지는 전송 시 서명값을 포함하므로 수신자는 메시지의 무결성에 대한 확인이 가능하다. 또한 RSU에 저장된 키 Table이 공격자에게 노출되지 않는다면 차량과 RSU의 메시지에 포함된 서명값은 보안이 유지된다. 핸드오버 시에는 RSU간에 차량의 키값이 RSU의 공개키값으로 암호화되어 전송되므로 차량의 키는 안전하다.

4.1.3. 가용성

위치기반 ID기법을 통해 기존 프로토콜에 존재했던 핸드오버의 문제점을 해결되며 차량의 도메인전이를 안전하고 간단하게 수행된다.

4.1.4. 익명성

RSSI기반 위치, 속도 그리고 가속도 개념을 이용하여 특정차량을 정확하고 빠르게 확인 가능하다. 이는 공격자가 메시지 분석시 ID값이 메시지에 포함되지 않으므로 어떤 차량의 메시지인지 확인하는 것을 불가능하게 한다.

4.2. 효율성

4.2.1. 계산량

제안된 기법은 기존의 기법의 k-anonymity를 사용하지 않으므로 해쉬연산에 대한 전수 조사 연산을 하지 않아도 된다. 대신 RSSI를 통한 거리 및 속도 연산을 통해 ID를 생성하게 된다. 해당 연산은 표 2의 간단한 수식을 통해 계산이 가능하여 k-anonymity를 통해 해시전수조사을 수행하지 않아도 됨으로 효율적이다.

표 6. RAISE, Jung과 제안된 기법의 계산량
Table 6. Complexity of RAISE, Jung and proposed techinque

	RAISE	Jung. et. al	제안된기법
키교환 회수(RSU-V)	$D \times r$	D	D
해쉬통합 (RSU)	$H \times k \times n$ $H \times n$, HAggt의 서명 계산	$H \times k \times n$ $H \times n$, HBCAggt의 서명 계산	$R \times n \times 2$ $H \times n$, HBCAggt의 서명 계산
검증 (V)	HAggt의 서명, 검증, H	HBCAggt의 서명, 검증, H	HBCAggt의 서명, 검증, H

D : Diffie-Hellman
H : 해쉬함수
n : 메시지의 개수
k : 키 테이블에 등록된 개수
r : RSU의 개수
R : RSSI를 통한 거리 및 속도 계산

4.2.2. 정확도

본 논문에서 제시한 기법의 효용성을 판단하기 위해 RSSI값을 통한 거리측정기법의 오류범위를 계산하였다. 그림 12는 거리에 따른 RSSI값의 변화를 나타낸다. RSSI값은 거리가 증가함에 따라 감소하게 된다. 그림 13은 그림 12에 나타난 RSSI값의 표준편차를 나타내고 있다. 표준편차의 값은 3에서 6사이의 값을 유지한다. 현재 표준편차의 평균은 4.1이고 RSSI값은 거리의 차가 2m일 경우 4.2이다 따라서 RSSI값은 2m이상일 경우 RSSI값의 표준편차의 오류를 벗어나게 되므로 차량간의 거리가 2m이상일 경우 정확한 거리판단이 가능하다. 또한 RSU와 RSU_Assistnat의 정보통합을 통해 RSSI 기반 거리 측정시 발생가능한 오류의 확률을 반으로 줄였다.

본 논문에서는 자동차에 대한 실용적인 적용을 위해 실제 소형차를 기준으로 하여 예시를 들었다. 소형차의 판단기준은 길이 3.6m, 너비 1.6m, 높이 2.0m 이하인 차량을 의미한다. 또한 표준 도로의 폭은 최소 2.75m이상을 유지해야 한다. 따라서 차량과 차량사이에는 2.75m를 최소한 유지한다. 이 값은 RSSI를 통한 위치판단의 오류범위를 벗어난다.

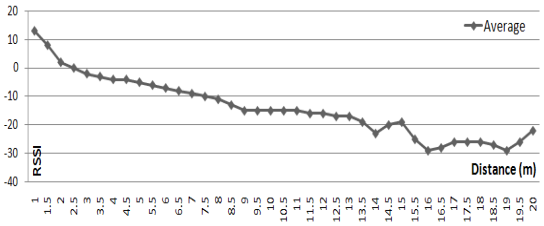

그림 12. 거리에 따른 RSSI
Fig 12. RSSI depending on distance

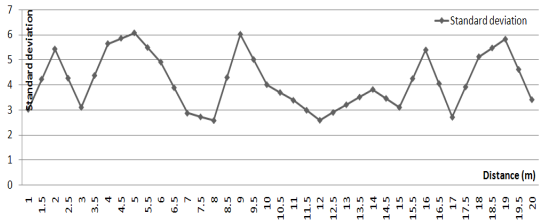

그림 13. 거리에 따른 표준편차
Fig 13. Standard deviation depending on distance

Ⅴ. 결 론

본 논문에서는 차량의 메시지 전송 시 사용되는 신호의 세기를 이용한 차량의 ID 판단의 신뢰성을 높이기 위해 RSU와 RSU_ASSISTANT의 통합 거리계산 알고리즘과 도메인 이동시 안전하게 키가 전달되는 핸드오버 프로토콜을 정의하였다. 이를 통해 기존 프로토콜의 k-anonymity를 통한 메시지 검증 시 해시연산의 전수조사로 인한 계산부하를 줄였으며 이동성으로 인해 발생하는 차량 도메인의 변경 시 발생하는 문제점을 해결했다. 프로토콜은 보안 요구사항인 무결성, 기밀성, 사용자 인증 그리고 익명성을 보장한다. 따라서 기존 프로토콜에 비해 VANET상에서 보다 효율적인 보안통신이 가능하다.

참고문헌

[1] 조영준, 이현승, 박남제, 최두호, 원동호, 김승주, “VANET에서의 보안 기술동향”, 한국정보보호학회, 제19권 제1호, pp.134-142, Feb, 2009

[2] 정석재, 유영준, 백정하, 이동훈, “차량 밀집환경에서 안전하고 효율적인 V2V 메시지 인증기법”, 한국정보보호학회, 제20권 제4호, pp. 41-52, Aug, 2010.

[3] B. Bloom. ″Space/Time Trade-offs in Hash Coding with Allowable Errors,″ Communications of ACM, vol. 13, no.7, pp.422-426, Jul, 1970.

[4] C. Zhang, X. Ling, and P-H. Ho, ″RAISE: An Efficient RSU-aided Message Authentication Scheme in Vehicular Communication Networks,″ in Proc. IEEE ICC 2008, Beijing, China, pp. 1451-1457, May. 2008.

[5] Shaohe Lv and Xiaodong Wang and Xin Zhao and Xingming Zhou, “Detecting the Sybil Attack Cooperatively in Wireless Sensor Networks,” pp. 442-446, Dec, 2008.

[6] Won Seok Choi, Jong Wook Nam and Seong Gon Choi, ″Hop State Prediction Method Using Distance Differential of RSSI on VANET,″ Networked Computing and Advanced Information Management, 2008. NCM’08. Fourth International Conference on, pp. 426-431, Sep, 2008.

[7] W. Diffie and M. E. Hellman, "New Directions in Cryptography," IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644-654, Nov. 1976.

저자소개

서화정(Hwa-jeong Seo)

2004.3～2010.2 : 부산대학교 정보컴퓨터공학과 학사
2010.2～현재 : 부산대학교 컴퓨터공학부 석사

※관심분야 : 정보보안, RFID/USN, 암호 이론, VLSI 설계

김호원(Ho-won Kim)

1989. 3～1993. 2 : 경북대학교 전자공학과 학사
1993. 3～1995. 2 : 포항공과대학교 전자전기공학과 공학석사
1995. 2～1999 . 2 : 포항공과대학교 전자전기공학과 공학박사
1998. 12～2008. 2 : 한국전자통신연구원(ETRI) 정보보호연구단 선임연구원 / 팀장
2008. 3～현재 : 부산대학교 정보컴퓨터공학부 조교수

※관심분야 : 스마트그리드 보안, RFID/USN 정보보호 기술, PKC 암호, VLSI 설계, embedded system 보안